| NODIS Library | Organization and Administration(1000s) | Search |

NASA Procedural Requirements

NPR 1600.1
Effective Date: November 03, 2004
Expiration Date: November 03, 2014

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change | (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

Appendix M: Designation of Public Trust Positions and Investigation Requirements

A. Public Trust Designation Model

Introduction. Proper position designation is the foundation of an effective and consistent suitability program. It determines what type of investigation is required and how closely an individual is screened for a position. Additionally, as the level of authority and responsibility of a position become greater, character and conduct become more significant in deciding whether employment, continued employment with the Federal service, or accesses granted or required under a NASA contract would protect the integrity and promote the efficiency of the Government.

Through this Appendix and Chapters 2, 3, and 4 of this NPR, NASA has established a consistent and uniform method for determining the risk level of civil service positions and functions and for those positions occupied by NASA contractor personnel. Because contractors play such a major role in all areas of Agency operations, their reliability and suitability are of equal importance. This Appendix meets the requirements established by the Office of Personnel Management (OPM) for federal employment and provides the appropriate mechanism for position risk designation for NASA contracts and contractor personnel.

Position Designation Records. Each NASA Center shall complete and maintain the Position Designation Record or its equivalent for each Agency civil service position and will also maintain similar records for NASA contractor personnel.

- Center personnel offices shall maintain the record of Public Trust suitability designations for all NASA civil service employees. These Position Designation Records are subject to review by OPM during periodic appraisals of NASA suitability programs, or on a case-by-case basis, to assure that NASA is considering all pertinent factors when designating positions relative to the integrity and efficiency of the service.
- Center security offices shall maintain copies of civil service designations and shall establish and maintain records for all contractor personnel, as well. These records will be subject to review during security program audits and reviews.

The Risk Designation System. The Risk Designation System is divided into three parts:

- *Program Designation.* The Agency identifies both the impact and scope of an Agency program as related to the integrity and efficiency of the service. This determines the "program designation."
- *Position Risk Designation Points.* The Agency determines the degree of risk that a position poses to the Agency or an Agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total "position risk designation points" for a position.
- *Position Designation.* The Program Designation and Position Risk Designation Points are applied to determine the risk level "position designation."

At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation shall result in a higher risk level, the other steps may not be needed.
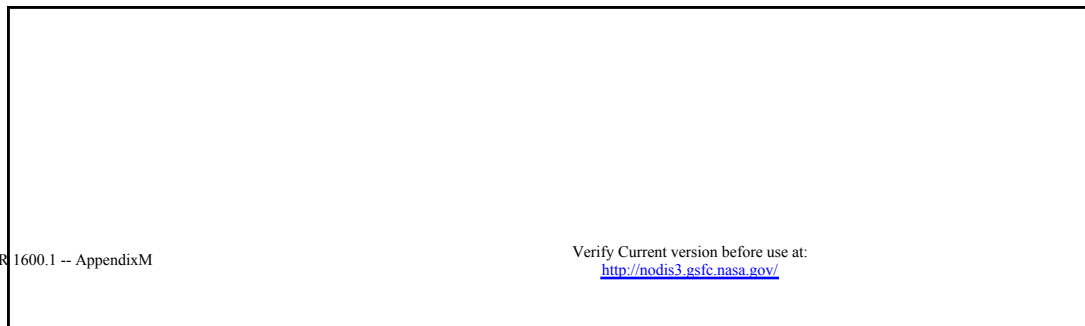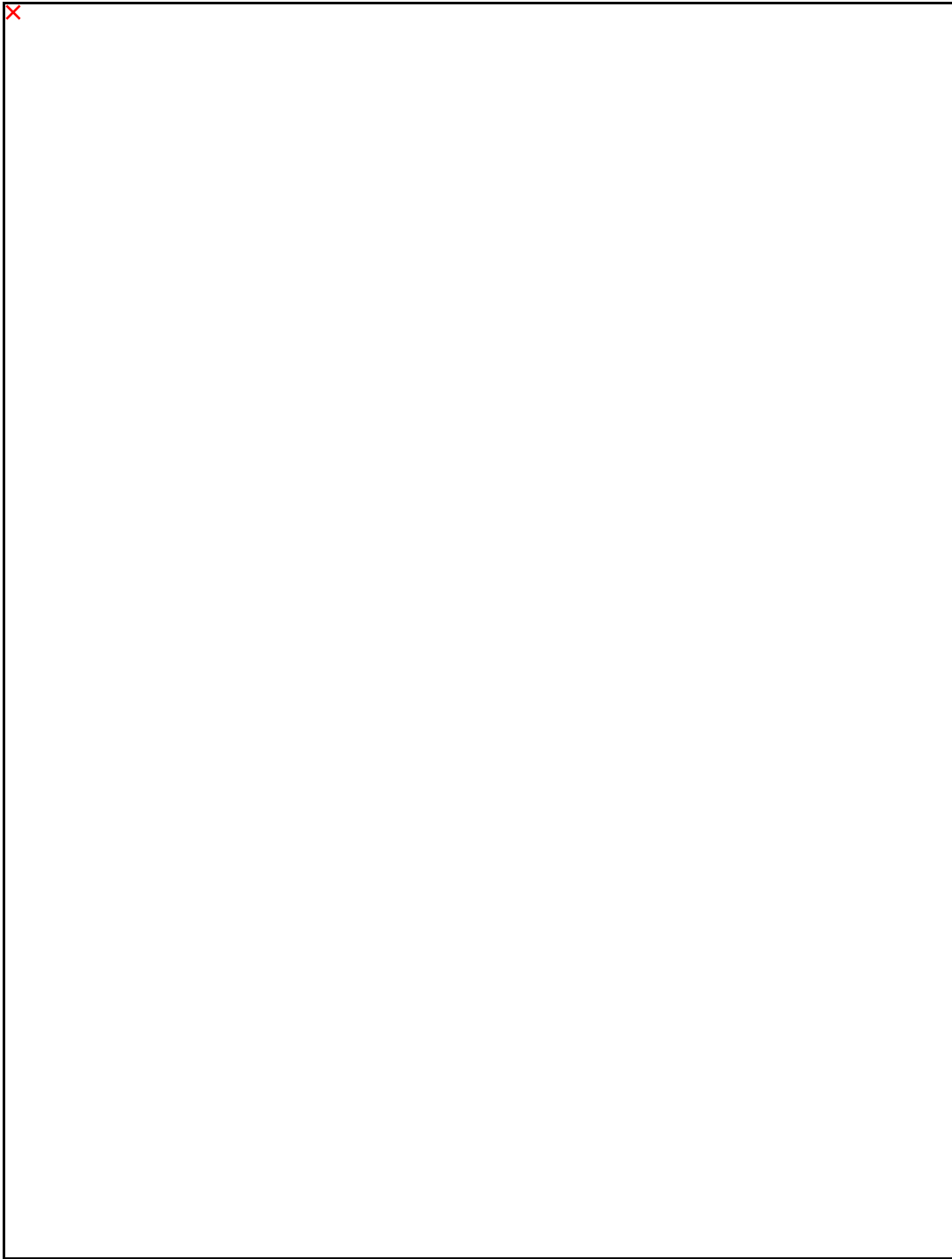
Figure 1

FILLING OUT THE POSITION DESIGNATION RECORD

Program Designation

? Program Designation. The appropriate management official identifies both the impact and scope of a program as related to the integrity and efficiency of the service. This determines the "program designation."

Use these steps and Table 1 on the next page to complete part I - "Program Placement"

1) Impact on the Integrity and Efficiency of the Service: Identify the impact description in the IMPACT column of Table 1 that best describes the program. If there is a question regarding the designation of program at one of two impact descriptions (such as whether it is SUBSTANTIAL or MODERATE), the decision must be based on the best interests of the mission.
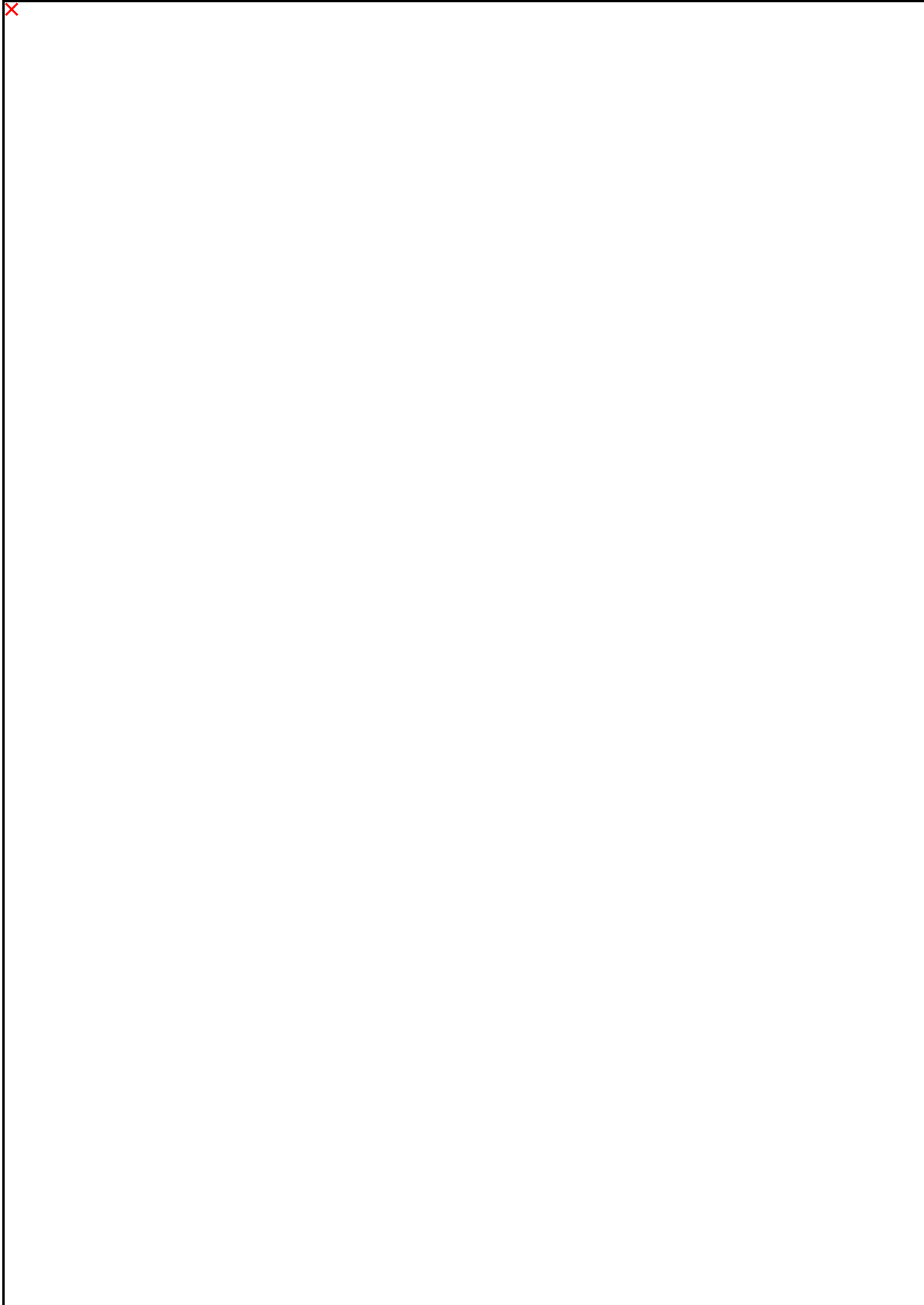
2) Scope of Operations in Terms of the Integrity and Efficiency of the Service: Identify the scope of operations described in the four SCOPE OF OPERATIONS columns of Table 1.

3) Determining Program Designation: The box at the intersection of the IMPACT row and SCOPE column identifies the program designation.

Examples:

(1) SUBSTANTIAL IMPACT and (2) MULTIAGENCY SCOPE = (3) SUBSTANTIAL Program Designation.

(1) LIMITED IMPACT and (2) WORLDWIDE SCOPE = (3) MODERATE Program Designation.

Designating Position Risk Points

? Position Risk Designation Points. The appropriate management official determines the degree of risk that a position poses to the Agency or an Agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total "position

risk points" for a position.

Use these steps and Table 2 on the next page to complete part II - "Position Risk Designation Points"

1) **Risk Factors and Degree of Risk:** Using a position description, or any documented information describing the duties and responsibilities of a position, evaluate each RISK FACTOR described at the top of Table 2 in terms of the DEGREE OF RISK described in the first column.

2) **Risk Factors and Points:** Assign points (7-6-5-4-3-2-1) to each risk factor to numerically reflect the DEGREE OF RISK. (The greater the degree of risk, the higher the point value assigned to the risk factor.)

3) **Total Points:** After points are assigned to all five risk factors, total the points. The result is a numerical representation of the relative degree of risk a position poses to the Agency or an Agency program (as related to the integrity and efficiency of the service).

Example:

SUBSTANTIAL "Degree of Public Trust" = (2) 5 points
SUBSTANTIAL "Fiduciary (Monetary) Responsibility" = (2) 4 points
LIMITED "Importance to Program" = (2) 1 point
MODERATE "Program Authority" = (2) 2 points
MODERATE "Supervision Received" = (2) 3 points

The total Position Risk Designation Points (5+4+1+2+3) = (3) 15
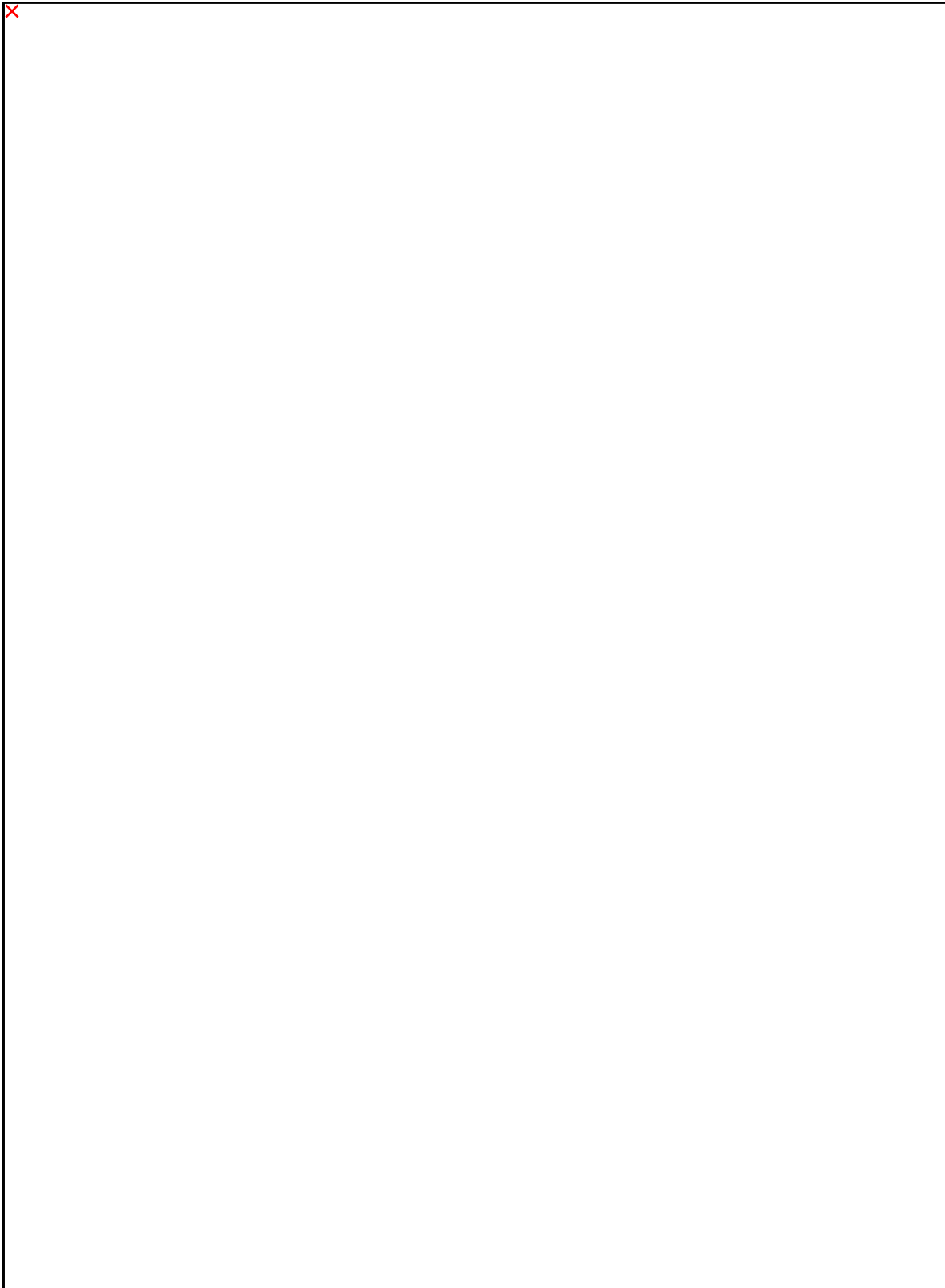
Position Designation
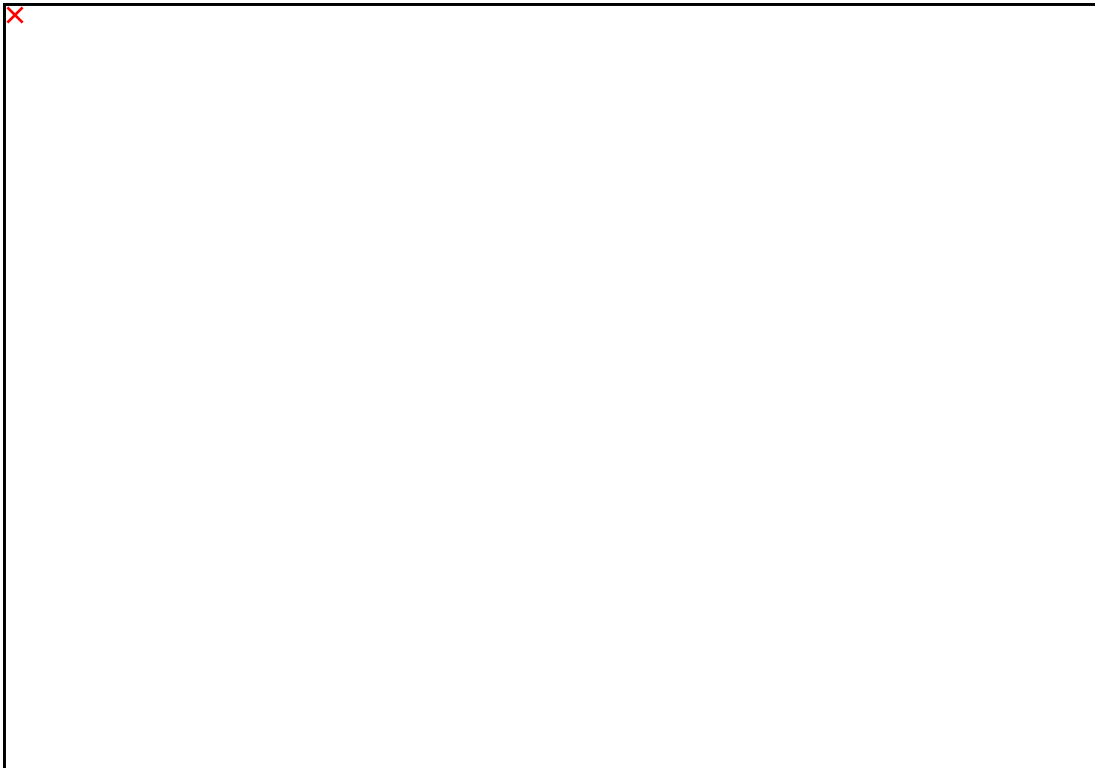
? ***Position Designation.*** The Program Designation and Position Risk designation Points are applied to determine the risk level "position designation."

At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation shall result in a higher risk level, the other steps may not be needed.

The results of part I, Program designation, and part II, Position Risk Designation Points, are next applied to Table 3 to determine the risk level of the position and to pair the risk level with the recommended minimum level of investigation for the position. The investigation recommendations are not intended to restrict Centers from conducting a more comprehensive investigation than

that prescribed, when such investigation is considered warranted.

TABLE 3

Minimum Investigative Requirements. The following are the **required** minimum levels:

LOW RISK - **NACI**
MODERATE RISK - **MBI**
HIGH RISK - **BI**

However, OPM recommends the levels shown in Table 3, above.

Adjustments: Some positions, by the very nature of the duties and responsibilities of the program or the position, may require designation at a certain level of risk. Final adjustment in the designation process must take into account unique factors specific to positions and the organizational need for uniformity of operations. Adjustments serve to raise the risk level designation of a position or convert the designation from a risk level to a sensitivity level. As a consequence, the level of investigation is often raised.

Uniqueness. Some factors that can cause a uniqueness adjustment, that are unique and are not fully accounted for in the program or position designation system, are listed here:

- Special investigative or criminal justice duties.
- Positions requiring possession and use of a firearm.
- Significant public health duties.
- Significant public safety duties.
- Access to or control of highly sensitive but unclassified information.
- Access to sensitive financial records.
- Potential for realizing significant personal gain.
- Control of an automated monetary system (such as key access entry).
- Few-of-a-kind positions with special duties (such as Special Assistant to Agency Head).
- Support positions with no responsibilities for preparation or implementation of Public Trust program policies and plans but involving regular contact with, and ongoing knowledge of, all or most of such material (such as Budget Analyst, Special Assistant).
- Any of the criteria appearing in 5 CFR 732 or E.O. 12968.
- Computer-ADP; any of the criteria under OMB Circular A-130 or Federal Information Security Act (FISMA) of 2002.
- Any other factors the Agency thinks relevant (these must be documented).

Uniformity. There may be a clearly indicated need for uniformity in position designations, because of authority level or program designation level; two examples that can cause adjustment are listed here:

- The NASA Administrator may adjust position designations at the same authority level to assure uniformity within the Agency (for example, managers of major Agency programs at the same level of authority may be designated at the same level of risk).

- If the NASA Administrator determines the designation levels of programs override and negate any specific risk considerations associated with individual positions within NASA or a NASA program, he/she may designate all positions within a program at the risk level required to protect the integrity and best promote the efficiency of the service.

Only after analysis of the position in terms of uniqueness and uniformity should any adjustment decision be made for FINAL DESIGNATION. FINAL DESIGNATION could be any one of the following:

See adjustment examples on the next page.

B. COMPUTER/ADP POSITION RISK LEVELS

The Computer/ADP position risk levels are an integral part of the Risk Designation System. Determining a Computer/ADP position risk level is an adjustment factor for both uniqueness and uniformity and tends to raise the risk level designation. The three Computer/ADP position risk levels are described in the following table; in determining position designation for any position with Computer/ADP duties, apply these definition considerations:

✗
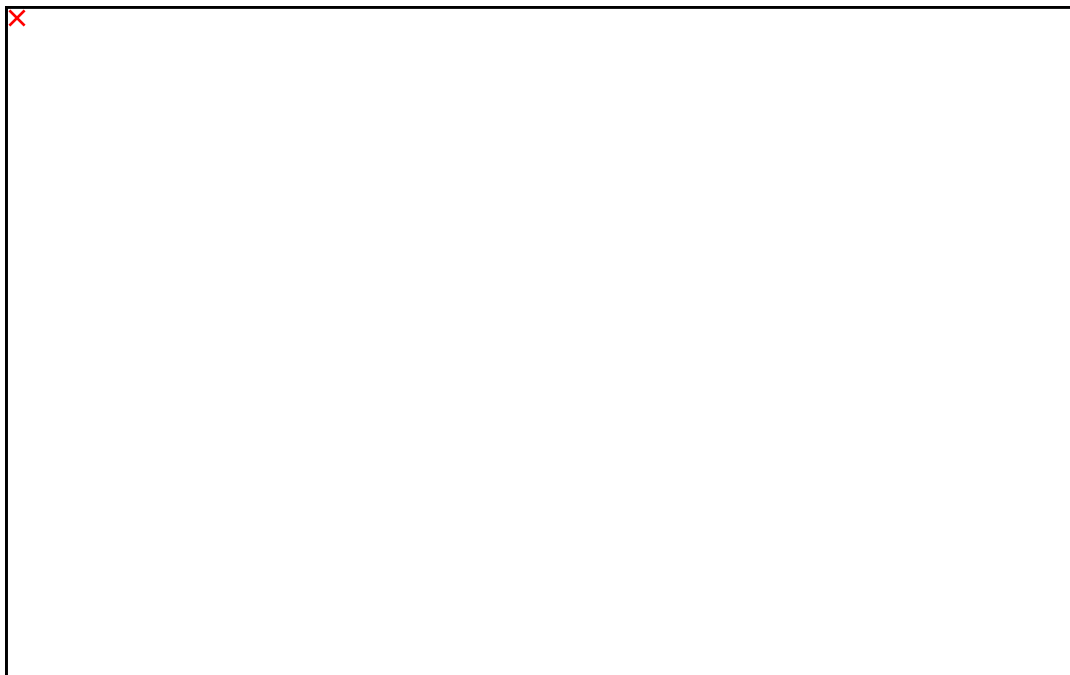
Risk Levels.

High Risk: Includes any position at the highest level of risk to the Computer/ADP system. Such positions may involve:

- Responsibility for the development, direction, implementation, and administration of Agency computer security programs, including direction and control of risk analysis or threat assessment.

- Significant involvement in life-critical or mission-critical systems.

- Responsibility for preparing or approving data for input into a system which does not necessarily involve personal access to the system, but which creates a high risk for effecting grave damage or realizing significant personal gain.

- Assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to insure the integrity of the system.

- Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, or management of systems hardware and software.

- Access to a system during the operation or maintenance in such a way to permit high risk for causing grave damage or realizing a significant personal gain.

- Other positions as designated by the NASA Administrator that involve high risk for effecting grave damage or realizing significant personal gain.

Moderate Risk: Includes positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the High Risk level to insure the integrity of the system. Such positions may involve responsibility for systems design, operation, testing, maintenance, or monitoring that is carried out under technical review of higher authority at the High Risk level, to insure the integrity of the system. This level includes, but is not limited to:

1. 1. Access to or processing of proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts.

2. 2. Accounting, disbursement, or authorization for disbursement from systems with amounts less than $10 million per year.

3. 3. Other positions designated by the NASA Administrator that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in High Risk positions.

Low Risk: Includes all Computer/ADP positions not falling into one of the above risk levels.

In order to establish uniformity and objectivity, management officials must make Computer/ADP risk designations in a systematic manner. Since positions can involve determinations of risk level for both suitability and Computer/ADP, the higher of the two risk levels is used for final position designation.

C. NATIONAL SECURITY POSITION SENSITIVITY LEVELS

All positions with National Security duties and responsibilities must have a sensitivity level designation to assure the appropriate level of investigative screening is done to comply with E.O. 10450 and E.O. 12968. Under 5 CFR Part 732, a sensitive position is defined as "...any position within a department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the National Security." Consequently, sensitivity level designation is based on an assessment of the degree of damage that an individual could cause to the National Security. There are three sensitivity levels: Special-Sensitive, Critical-Sensitive, and Noncritical-Sensitive, defined in the table that follows:

SPECIAL-SENSITIVE
(SS)

Any position that the NASA Administrator determines to be at a higher level than Critical-Sensitive due to special requirements that complement E.O. 10450 and E.O. 12968 (such as Director of Central Intelligence Directive [DCID] 6/4 that sets investigative requirements and access to Sensitive Compartmented Information [SCI] and other intelligence-related Special Sensitive information).

CRITICAL-SENSITIVE
(CS)

Potential for exceptional or grave damage to the national security.

Positions that involve any of the following:

- Access to Top Secret classified information;
- Development or approval of war plans, or plans or particulars of future, major, or special operations of war, or critical and extremely important items of war;
- National security policy-making or policy-determining positions;
- Investigative duties;
- Issuance of personnel security clearances;
- Duty on personnel security boards; and
- Any other positions related to national security requiring the same degree of trust.

NONCRITICAL-SENSITIVE
(NCS)

Potential for significant or serious damage to the national security. Positions that involve any of the following:

- Access to Secret or Confidential classified information, or
- Duties that may directly or indirectly adversely affect the national security operations of the agency or the government.

NOTE: The designation of Non-Sensitive is not shown in the table because a Non-Sensitive position is the same as a Low Risk position; both require the same level of investigation, a NACI.

Apply the sensitivity levels described in this part as an Adjustment in the Risk Designation System to arrive at a final designation. This Appendix references 5 CFR 732 as one of the uniqueness adjustment factors. The reference pertains to Subpart B of the section on "Sensitivity level designations and investigative requirements." The table on the previous page shows the sensitivity level designations, as well as their definitions and examples of the types of duties and responsibilities that correspond to the Critical-Sensitive and Noncritical-Sensitive levels. Centers shall consider the information displayed in this table when deciding if a position must have a sensitivity designation.

Sensitivity level designations override Public Trust (i.e., HR and MR) designations due to the national interest or security. However, the basic risk level of a position needs to be determined first. If National security duties and responsibilities are no longer a part of a position, the position then reverts to its Public Trust designation. Additionally, if the Public Trust risk level designation requires a higher level of investigation than the National security sensitivity level, the higher level of investigation must be conducted. For example, if the basic position designation is HR, but the position requires Secret access, the position would have an adjusted designation of Noncritical-Sensitive because of the Secret access. The investigation required would be a BI for the HR position, and not an ANACI for the Noncritical-Sensitive designation due to Secret access. The higher level of investigation prevails because of the more intensive screening required of an HR position, a BI investigation being a higher level of investigation than an ANACI.

5 EXAMPLES:

DISTRIBUTION:
NODIS